# The Cambridge Community Remote Station Project

**The Cambridge Community Remote Station Project started in October 2014. Our goal was to establish an HF amateur radio station that could be operated remotely by club members of Camb-Hams and CDARC. This would stimulate on-the-air activity associated with club activities such as training, operating, public demonstrations and club evenings. At the same time the project would provide a series of diverse technical challenges to interest the more technically minded members since their skills would be necessary to bring such a project to a successful reality.**

PHOTO 1: Bob, G3PJT operating on 40m from a corner of RSGB HQ. All he needed was the equipment you see plus a power socket and Wi Fi access.

## Rationale

Many radio amateurs are finding that modern society does not sit well with the need to operate on the air freely and effectively.

In some cases amateurs cannot operate at all due to

- locally generated noise that effectively 'deafens' their receivers due largely to emissions from domestic and industrial devices,
- the compact urban environment and restrictive planning regulations that severely limit the possibility for antennas both at HF and VHF,
- EMC problems with neighbours' electronic devices, of which there is a plethora these days.

The amateur population is ageing and some thus find themselves forced into sheltered or restricted accommodation with little or no opportunity for amateur operation even though this would be one of the few pastimes they could still enjoy. The same situation applies to those who are housebound for other reasons. Many, especially the young, find themselves in rented accommodation or in apartments with tight restrictions on outdoor antennas.

Often when faced with these situations many 'would-be-active' amateurs just give up and become inactive or exit the hobby entirely. This is a very unfortunate outcome that the radio amateur community should try and avoid if at all possible.

However many of us do have internet broadband even in the most restricted environments and we believe this provides us with an opportunity to create a new type of 'club' station that might allow us to break out of this situation. At the same time it even might provide a lower cost entry point for those entering or re-entering our hobby.

The quality and coverage of broadband services, both wired and 3G/4G based, is improving rapidly and this provides the infrastructure for an effective remote controlled amateur radio system.

This article describes our project designed to address some of these issues in the context of a club station. The project comprises a dedicated and secure HF station that can be accessed with a portable control package that clubs and their members can borrow and use. We believe it is important that the user has proper feel of operating a radio and for that reason attention has been given to the ergonomics of the system – it has to feel like you are using a 'real radio'.

For these reasons this project is based on the Elecraft K3 and the Microbit Remote Rig units. The system has been established successfully and basic tests have shown that the concept is viable.

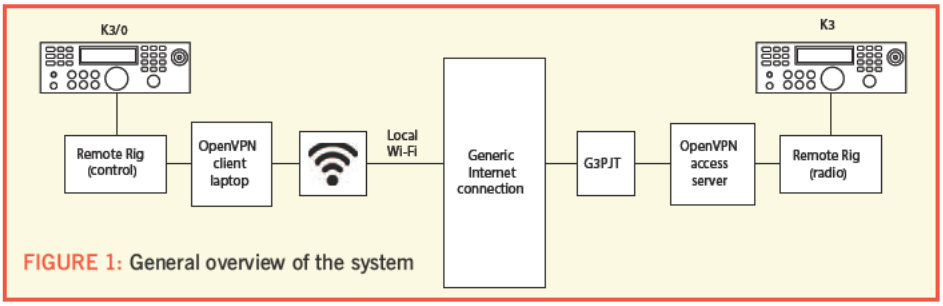


FIGURE 1: General overview of the system

PHOTO 2: The remote station is compact yet powerful and can be completely controlled from anywhere there's a suitable internet connection.

PHOTO 3: The complete 'operator' setup comprises a laptop, Microbit Remote Rig 1258 mk II and an Elecraft K3 front panel. A Morse key can, of course, be added.

## System

Stated simply, the system works as shown in **Figure 1**. A remote radio, sited in a suitably quiet radio environment and connected to broadband, is controlled remotely by a user with a dedicated terminal unit and a broadband connection. The remote radio can operate on a number of HF (or VHF) bands and is completely under the control of the user. By this we mean that it can be turned on and off, the operating frequency can be tuned, the mode and filters selected, the power level adjusted etc. The radio, and any accessories like rotators and power meters, have to be able to be controlled through software, but many modern radios and accessories have this facility. Such a system has to have a number of safeguards built in order to meet regulations and above all should fail-safe into a locked down or quiescent state.

One of the challenges relates to broadband access and the varying quality and firewall implementations found in public Wi-Fi arrangements and on restricted networks. Unlike many remote control applications where both ends of the network are under the radio amateur's direct control, we must accept that one end point will commonly be managed by a third party and cannot be changed.

PHOTO 4: You really can operate from anywhere!

## The remote station

The remote HF station at G3PJT (shown in **Photo 2**) includes an Elecraft K3, a KPA500 amplifier, a set of antennas covering 80m to 15m and a rotator. This station is controlled by a Microbit Remote Rig 1258 mk II that in turn is connected to the router/modem and a dedicated broadband line. **Figure 2** shows the interconnections.

The K3 and the KPA500 amplifier are linked together such that the amplifier is under the control of the K3 for operating band selection, power control and fault reporting. Antennas are selected by the K3 via a 5 way antenna switch and cannot be selected by the user. This is to ensure that the K3 or the amplifier cannot operate into an incorrect antenna. The Remote Rig unit controls the state of the K3 and processes audio to and from it. In addition it controls the mains power sequencer. The Intel NUC mini-PC hosts software for the Virtual Private Network (VPN) and for the rotator. See page 22 for more details on this.

When the remote station is not operating we needed to have it positively powered off. Many remote systems are part powered up to allow a warm start. In our case only the broadband modem/router, the Remote Rig unit and the NUC are powered up at all times (on a UPS for stability). When a connection request is received by the Remote Rig this triggers a request to the mains power sequencer and this enables power to the radio PSU and then turns the K3 on in the proper order. When the connection is broken the reverse occurs thus ensuring a smooth switch on and off for the remote radio. This facility also ensures safe shut down in the event of loss of the connection. An instruction from a iPhone-based 'kill switch' can be used to shut the station down in the event of serious problems. Tests have shown this system fails safe to shut down as is required.

A standard broadband modem and router completes the station. Early trials showed that it is best to have a robust broadband connection so a dedicated, un-contended line with a performance of 40Mb/s down and 10Mb/s up with a monthly usage cap of 100GB has been installed. This has proven to be plenty of capacity.

## G3PJT Remote Station network description overview

During our testing of the Microbit Remote Rig system, we were surprised to find a variety of problems connecting the same setup between one broadband connection and another. For example, on some connections the system would connect easily, while on others it would resist all attempts to connect. In those cases, only moving the Remote Rig fully into the Demilitarized Zone (DMZ) thus exposing it directly to all internet traffic would succeed. This is not a desirable arrangement.

This pattern would vary from one ISP to another. Usually, after probing the traffic involved, some explanation could be found (eg variations in broadband router firmware and other policy or security extensions).

One of the main principles of the G3PJT remote station is that it may be connected to from a wide range of locations, including via 3G/4G mobile phone network modems, public Wi Fi and the like. Additionally, it cannot be assumed that there will be time or expertise available to diagnose network problems in depth. The client end that controls the station will often be using a network that is not under our direct control (and will often require accepting checkbox terms and conditions using 'captive' portals and the like). It is essential to have a solution that connects readily and reliably, since obtaining local IT help to make changes is likely to be impossible.

We decided that the best solution would be to create a Virtual Private Network (VPN) network layer between the client and the server, and to combine the Remote Rig with a laptop that provides routing of network traffic over the VPN transparently. The wide range of Wi Fi systems found in venues strongly prefers the use of a laptop, keyboard and mouse to get connected, so this also conveniently solved the problem of getting connected to the internet!

To be clear, the desired benefit of the VPN is to standardise the configuration of the Remote Rigs. In this concept there is never a need to login and edit settings on either the control end or the radio end. The laptop automatically establishes a VPN network connection when the user connects it to an available Wi Fi signal and presents a route via the VPN on its Ethernet port. Usually, within 30 seconds of booting the laptop, the user will be able to be on the air. Site to site network variations require no special handling provided the internet connection can support an OpenVPN client and TCP/UDP traffic flows with reasonable latency.

### Server (radio)

The server is an OpenVPN Access Server, installed in the form of a virtual appliance (see https://openvpn.net/index.php/access server/overview.html). A simple web based UI is available as standard, or a more adventurous project using the underlying OpenVPN tools directly and text configuration files is also possible.

In the G3PJT station, the OpenVPN Access Server is running on a VMWare ESXi hypervisor, so that a single compact Intel NUC can be used for a variety of purposes. A dedicated PC to run the OpenVPN AS is probably not justified as it is a lightweight network service, so a suitable alternative would be to use a Raspberry Pi. OpenVPN is a standard package that is widely used with these devices.

TCP and UDP ports for the OpenVPN protocol are passed using NAT translation on the broadband router directly to the OpenVPN server on the private LAN. Clients that connect to the OpenVPN server are connecting to the public (WAN) IP address of the radio site, but after connecting they are provided with a local LAN IP address and route that allows them to access devices within the radio network. The OpenVPN server is essentially tunnelling them to that network while also encrypting all traffic in transit.

The OpenVPN server is connected to the same physical network segment as the Remote Rig at the radio end. The Remote Rig cannot be accessed directly from the internet, but traffic passing through the OpenVPN server can reach the Remote Rig. There are obvious security benefits to this arrangement when compared with exposing a Remote Rig directly to the internet.

Example network on the server (radio) side:

- Router IP: 80.90.100.110 [WAN]
- Router IP: 192.168.1.1 [LAN]
- OpenVPN Access server 192.168.1.2
- Remote Rig (radio): 192.168.1.3
- Remote Rig (radio) default gateway: 192.168.1.2

TCP/IP forwarding is enabled as standard in the OpenVPN access server, to allow it to act as a NAT gateway for client traffic terminated through the VPN. This is how traffic from the radio Remote Rig is returned to the control end.

### Client (control)

An inexpensive laptop running Linux runs a default installation of Ubuntu. This provides a convenient graphical interface for connecting to Wi Fi hotspots, using a web browser and common CLI tools such as ping, traceroute and so on.

The Wi Fi network on the laptop is dedicated to the local internet connection.

The Ethernet port on the laptop is statically configured with a private IP address. The network port on the Remote Rig is then connected directly to the laptop using a standard 100Mb/s Ethernet cable. On the Remote Rig, a static IP address is configured and the IP address of the laptop is the TCP/IP gateway, so that all traffic is passed first to the laptop for routing.

Example network on the client (control) side:

- Client laptop WAN IP: via DHCP from the available Wi Fi connection
- Client laptop static IP: 192.168.0.1
- Control Remote Rig static IP: 192.168.0.2
- Control Remote Rig gateway: 192.168.0.1

The laptop is installed with an OpenVPN client and a connection profile downloaded from the OpenVPN Access Server. The laptop triggers a VPN connection whenever a Wi Fi internet connection is available. As soon as the VPN connection is established, this has the effect of raising a TCP/IP route, and from that moment any traffic from the control Remote Rig on the Ethernet port is forwarded to the radio end, via the OpenVPN network.

TCP/IP forwarding is enabled on the Client laptop to allow it to act as a source NAT gateway for the Remote Rig. Traffic destined for the server (radio) network, 192.168.1.0/24, is routed by the laptop at 192.168.0.1.

In the example network described here, the control Remote Rig 192.168.0.2, will use 192.168.1.3, the radio Remote Rig's private IP address, as its partner. Neither Remote Rig is aware of the VPN.

Once connected, the normal procedure on the laptop is to ping the radio end's Remote Rig and ensure that a reasonably steady network connection is in place. This also validates that the VPN is up and functioning correctly. Additional remote servers (eg rotator control and CAT for the Elecraft radio) can also be tunnelled via the VPN. This has been working successfully and completes a fully secure, integrated remote operating environment that is highly portable.

### Conclusion

Using a VPN to route Remote Rig traffic has allowed the G3PJT remote station to be used from a wide range of different networks, including mobile phones, without any reconfiguration of the Microbit Remote Rig devices. Although somewhat involved to configure initially, once working there are no further changes to make. The VPN insulates the solution from any particular network requirements imposed locally. It is therefore a 'plug and play' solution with very few IT distractions.

Avoiding configuration changes arising during routine use of the station has significantly improved the reliability of the site. No user interaction with the Remote Rigs is necessary and so no changes are introduced inadvertently.

Using a VPN has also ensured that the service is completely secure. The client server authentication of the VPN connections provides ample audit possibilities that may be helpful when the site is put to use by multiple users in future, and it is hoped that the login credentials used will be linked to a local profile, to automatically prepare the station for the correct licence restrictions of the user.

## The control system

The control system shown in **Photo 3** and **Figure 3** comprises three units, a K3/0 mini, a Remote Rig controller and a Wi-Fi enabled, Linux laptop carrying the VPN access software. The K3/0 mini is the front panel of a K3 but does not include any of the RF components of a complete K3. In this application the display and controls of the K3/0 mirror the front panel and state of the remote K3.

## Using the system

A user first establishes a Wi-Fi connection using the Linux laptop and performs some basic tests of the broadband connection quality. Typically the speed required should be of the order of 2Mb/s down and 0.5Mb/s up but the main criterion is that of stability. A simple way of testing this is to measure the ping time to the remote station. This needs to be less than 500ms but typically is less than 60ms – but ideally this should not vary very much. When the K3/0 is turned on a connection is established to the remote radio in about 20 seconds. The radio can then be used just as if you were sitting operating the K3 at the remote site directly. It is also possible to create a perfectly adequate connection using a 3G/4G dongle and a TP Link mobile wireless router. This approach shows considerable potential for bypassing the various firewalls etc in public Wi-Fi or indeed the very limited connectivity and user capacity of many 'free' Wi-Fi systems found in pubs and restaurants.

Latency is always present but the Remote Rig system has features to minimise its effect and the CW side tone and keying for example is generated in a keyer in the control unit and not by the remote K3.

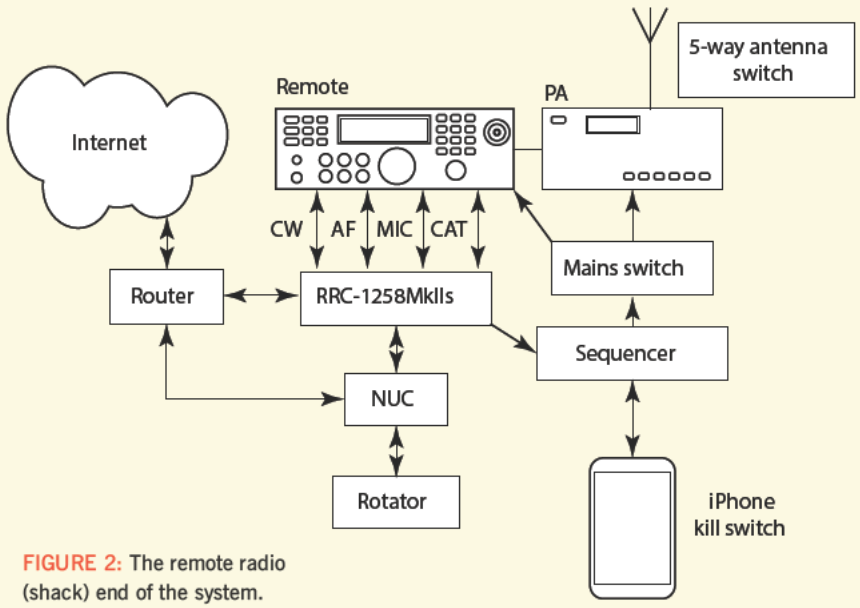


FIGURE 2: The remote radio (shack) end of the system.

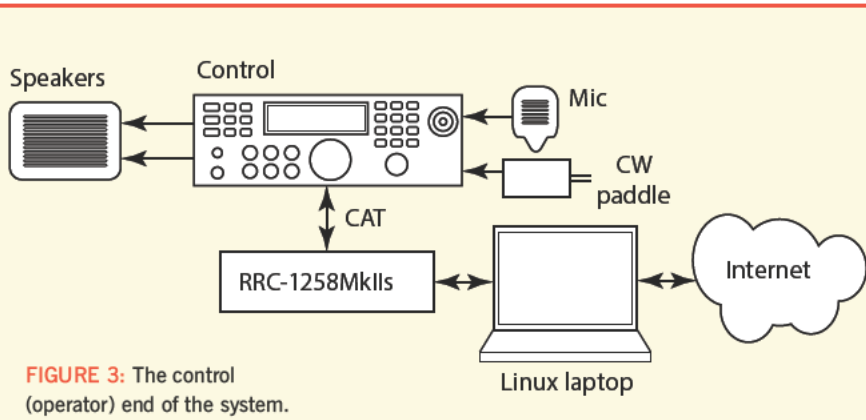


FIGURE 3: The control (operator) end of the system.

## Results and future

At the present time we have tested access from a number of different public internet and Wi-Fi access points such as village halls, libraries, private houses, pubs and even from RSGB HQ. Operation from private premises has always been successful but the same cannot be said for public Wi-Fi. There seem to be two main reasons, firewalls and limited capacity. For example at one pub the ping went from an acceptable 69ms when the pub was empty to 2000ms (2 seconds) when it was full of Camb-Ham members!

During the trial a number of local amateurs have used the system to very good effect, working DX, saying things like "that was fun!" and "I had a very good weekend of DXing!". Others enjoyed chatting on 40m from the low noise environment that "makes 40m sound like 2m"!

Of course the use of this station is subject to the amateur radio licence conditions and the RSGB will shortly publish some Good Practice guidelines for remote control operation.

We are now starting a series of demonstrations in local school clubs and other public locations. Clearly public demonstrations should become a great deal easier to organise and not be plagued with local noise, EMC problems and the need to erect outside antennas. We will be reporting our experiences in this aspect of the project later this year. We would like to hear from anyone who is working on the same sort of club project (via email to bob@g3pjt.com).

We believe that remote controlled operation is an important new opportunity for amateur radio clubs that will allow them to showcase our hobby in a whole new way and at the same time bring on-the-air activity into the club room and to the wider public.

## Acknowledgements

This project has been part funded by the RSGB Legacy Fund, funds which really got the project off the ground. Michael, G7VJR, Rob, M0VFC and Bob, G3PJT donated equipment and additional financial support to cover running costs and other equipment purchases, and were greatly helped by Gavin, M1BXF and Peter, M0DCV.

**WEBSEARCH**

Elecraft: www.elecraft.com/K3 Remote/k3 remote.htm

Microbit: www.remoterig.com/wp/

Bob Whelan, G3PJT
bob@g3pjt.com